Запропоноване ПЗ для встановлення захищеної сесії забезпечує перевірку, щоб доменне ім’я в сертифікаті відповідало тому домену, від якого йде запит на захищене з’єднання; сертифікат не був прострочений; сертифікації, що підписала сертифікат домену, входив до числа довірених Web-браузера.

Список літератури

1. Балакирский В.Б. Безопасность электронних платежей. Защита информації – Конфидент, № 5, 1996.
2. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. М.: Бином-пресс, 2002.
3. Бруно Л. Certificate Authorities: Кому Вы доверяете? Data Communications (Russian edition). № 3, 1998.
4. Галатенко В.А. Информационная безопасность. Обзор основних положений. Jet Info. № 1-3, 1996.
5. Галатенко В.А. Стандарты в области безопасности распределенних систем. Jet Info, № 5, 1999.
6. Галатенко В.А. Основы информационной безопасности. – М.: ИНТУИТ.РУ – "Интернет-университет информационних технологий", 2003.

УДК 004.056.55

В.О. Гаража
Науковий керівник – Дóренський О.П., викладач
Кіровоградський національний технічний університет

Створення архівів у файловій системі NTFS з розмежуванням доступу за допомогою алгоритму AES

Програми для стиснення даних почали розроблятися одночасно зі створенням перших персональних комп’ютерів, адже ще тоді постійно відчувалася недостача вільного місця на жорстких дисках. Як правило, користувачі стискують текстові документи, рідше – фотографії і відеодані, тому що в останньому випадку виграш у вільному місці виявляється зовсім невеликим. Процес створення архіву називають архівацією або упакуванням, а зворотній процес – розпакуванням або екстракцією [1].

Проте під час перенесення архівів портативними носіями або передачі їх мережею гостро постає питання безпеки заархівованої інформації. Тому задача забезпечення розмежування доступу до архівів є актуальною.

Метою роботи є розробка програмного забезпечення створення архівів у файловій системі NTFS з розмежуванням доступу.

Аналіз [2-5] показав, що серед найпоширеніших алгоритмів шифрування оптимальними з погляду специфіки їх роботи, рівня захисту та простоти імплементації є алгоритми AES та RSA. Водночас, симетричний алгоритм AES, наприклад, відповідно до дослідження [4], має значно кращу часову характеристику: якщо 1 Мб даних асиметричний RSA шифрує за 7,5 сек., то AES – за 0,51 сек. Тобто програмна реалізація криптографічних перетворень над даними на основі алгоритму AES є більш ніж в 10 разів швидша ніж при використанні RSA. Таким чином, алгоритм AES можна вважати доцільним для програмної реалізації з метою подальшого впровадження і використання, що є актуальною задачею. Також слід відзначити, що Rijndael стандарту AES – це швидкий і компактний алгоритм з простою математичною структурою, завдяки чому він є простим для аналізу під час оцінювання рівня захисту.

Отже, можна впевнено зробити висновок, що для розробки програмного забезпечення створення архівів у файловій системі NTFS з розмежуванням доступу є доцільним застосування саме алгоритму AES, відомого ще під назвою Rijndael [3].

Розробку ПЗ створення архівів у файловій системі NTFS з розмежуванням доступу за допомогою AES пропонується здійснити відповідно до розробленої структурної схеми, яку наведено на рисунку 1.

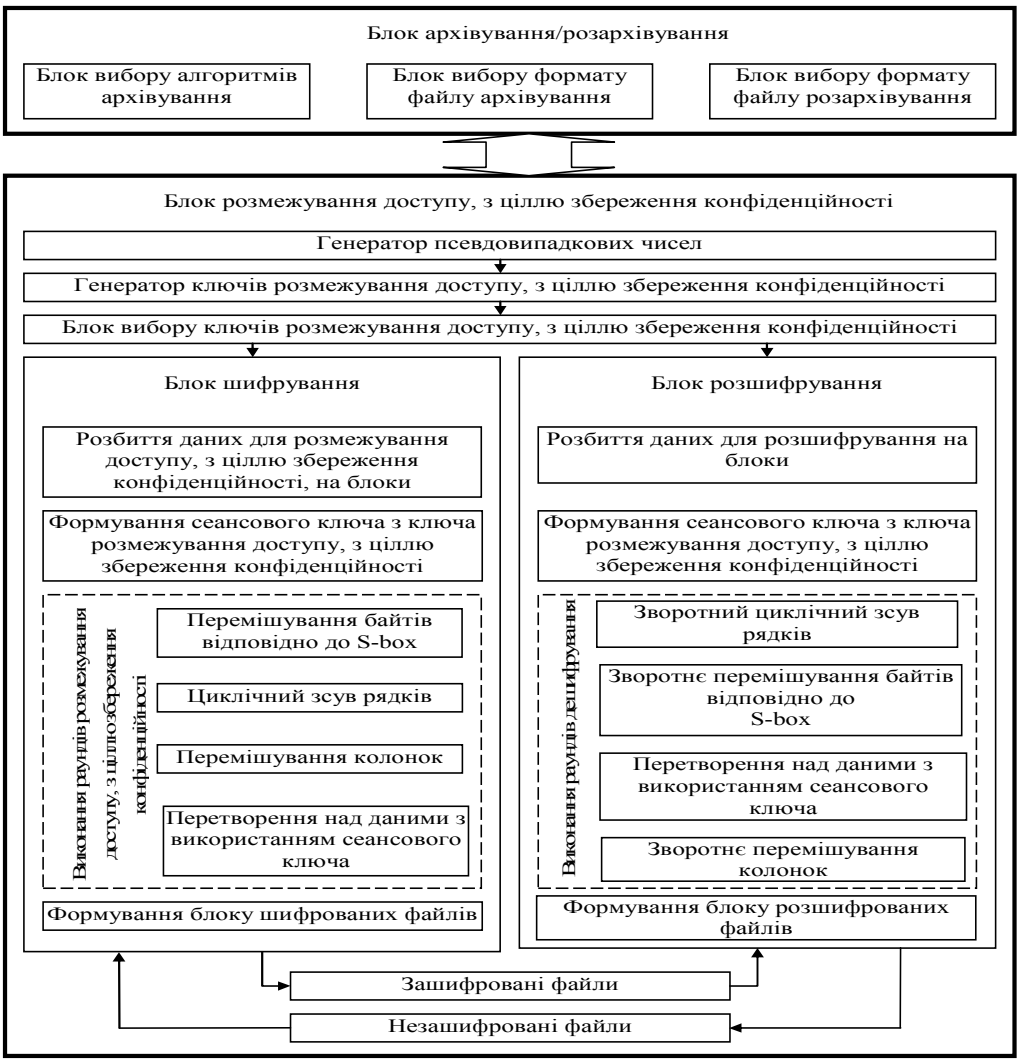

Рисунок 1 – Структуран схема ПЗ архівування у файловій системі NTFS з розмежуванням доступу за допомогою AES

У роботі [6] досліджено особливості програмної реалізації алгоритму AES. Слід відзначити, що AES є нетрадиційним блоковим шифром, оскільки не використовує мережу Фейштеля для криптоперетворень [7]. Він оперує 128-бітними блоками даних і довжиною ключа розрядністю 128, 192 або 256. Вхідні, проміжні і вихідні результати перетворень, що виконуються в рамках алгоритму, називають станами (state) [8], які можна представити матрицею 4xNb (Nb – кількість 32-бітних слів вхідного блоку), елементами якої є чотири рядки по Nb байт в порядку S00, S10, S20, S30, S01, S11, S21, S31 і т.д. Ключ шифрування, як і масив State [7], представляється прямокутним масивом (матрицею) з чотирма рядками.

До основних особливостей AES, який специфікує алгоритм Rijndael [5, 7], та його програмної реалізації можна віднести те, що він є симетричним блоковим шифром, який працює з блоковими даними довжиною 128 біт та використовує ключі 128, 192 і 256 біт (версії AES-128, AES-192, AES-256) [7]. Дослідження [5] показали, що однією з особливостей програмної реалізації і важливою перевагою з погляду криптостійкості, впровадженні й практичного застосування зазначеного алгоритму є

також те, що він може працювати і з іншими довжинами блоків даних та ключів. Хоча така можливість не входить до стандарту [3], проте вона може бути ефективно застосована на практиці.

Особливості програмної реалізації AES також випливають з особливостей самого алгоритма. Серед них, зокрема, слід відзначити нову архітектуру “Квадрат”, що забезпечує надшвидке “розсіювання” та “перемішування” інформації, при чому за один раунд перетворенню підлягає весь вхідний блок [5]. Крім того в алгоритмі застосовується байт-орієнтована структура, що під час програмної реалізації процесу шифрування забезпечує розробку на 8-розрядних мікроконтролерах. Варто відзначити одну з найважливіших особливостей AES: ефективна апаратна та програмна реалізація на різноманітних платформах. Зокрема важливим для програмної реалізації AES є те, що у структурі алгоритму закладена можливість паралельного виконання операцій, що на багатопроцесорних ЕОМ дозволить збільшити швидкість шифрування у кілька разів.

Список літератури

1. Тарасов О.В. Огляд та порівняльний аналіз методів стиснення інформації / О.В. Тарасов, Є.В. Онопко // Системи обробки інформації. – 2011. – Вип. 7 (97) – С. 64-67.
2. Бурачок Р.А. Використання симетричних алгоритмів шифрування при передаванні мультимедійних даних / Р.А. Бурачок, П.О. Гуськов, Р.І. Бак // Радіоелектроніка та телекомунікації. – 2012. – № 738. – С. 156-160.
3. Баричев С.Г. Стандарт AES. Алгоритм Rijdael / Баричев С.Г., Гончаров В.В., Серов Р.Е. // Основы современной криптографии. – М.: “ГЛ-Телеком”, 2002. – 247 с.
4. Дудикевич В. Б. Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв’язку / В.Б. Дудикевич, Ю.Л. Пархуць // Інформаційна безпека. 2011.–№1(5).–С. 83-87.
5. Фисун С.Н. Методика шифрования данных с использованием программно-методического комплекса VisualAES / С.Н. Фисун, А.И. Копылов // Радіоелектронні і комп’ютерні системи. – 2012. – № 5 (57). – С. 83-85.
6. Гаража В.О. Особливості програмної реалізації алгоритму AES / В.О. Гаража, О.П. Доренський // Актуальні задачі сучасних технологій: збірник тез доповідей Міжнародної науково-технічної конференції молодих учених та студентів, 19–20 грудня 2012 р., м. Тернопіль – Тернопіль: Вид-во ТНТУ ім. Івана Пулюя, 2012. – С. 184-185.
7. Основи захисту інформації: Навч. посібник. / [Смірнов О.А., Віхрова Л.Г., Осадчий С.І. та ін.]. – Кіровоград: РВЛ КНТУ, 2011. – 322 с.
8. Панасенко С.П. Алгоритмы шифрования. Спец. справочник / С.П. Панасенко. – СПб.: БХП Петербург, 2009. – 576 с.

УДК 004.4

Д.О. Давидов
Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи формування фільтрів від фішингу в мережі Internet

Найбільш розвинутою формою шахрайства в Інтернеті, безсумнівно, є фішинг. Зловмисники використовують перехоплювачі клавіатури, поштові повідомлення, складені за всіма правилами соціальної інженерії, спеціально розроблені сайти й інші засоби.

Усе більше винахідливими стають атакуючі, усе вище рівень їхньої підготовленості. Фішинг (phishing) – вид інтернет-шахрайства, що полягає в